May 15, 2024

Overall Rating - High

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that Cisco published security advisories to address vulnerabilities in multiple products. Included were updates for the following:

- Cisco Crosswork Network Services Orchestrator (NSO) CLI – multiple versions
- ConfD CLI – multiple versions

Technical Details

A vulnerability in the Tail-f High Availability Cluster Communications (HCC) function pack of Cisco Crosswork Network Services Orchestrator (NSO) could allow an authenticated, local attacker to elevate privileges to *root* on an affected device.
This vulnerability exists because a user-controlled search path is used to locate executable files. An attacker could exploit this vulnerability by configuring the application in a way that causes a malicious file to be executed. A successful exploit could allow the attacker to execute arbitrary code on an affected device as the *root* user. To exploit this vulnerability, the attacker would need valid credentials on an affected device.
Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2024-20366 CVE-2024-20326 CVE-2024-20389 CVE-2024-20326 CVE-2024-20389 CVE-2024-20391 CVE-2024-20369 CVE-2024-20256 CVE-2024-20257 CVE-2024-20258 CVE-2024-20392 CVE-2024-20394
- Cisco Crosswork Network Services Orchestrator Privilege Escalation Vulnerability
- Cisco Crosswork Network Services Ochestrator Vulnerabilities
- ConfD CLI Privilege Escalation and Arbitrary File Read and Write Vulnerabilities
- Cisco Security Advisories
-